R E P U B L I Q U E F R A N Ç A

PCT/FR2004/001849

0 1 SEP. 2004

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REÇU 22 NOV. 2004
OMPI PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 16 JUIL. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*02

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 010601

Réservé à l'INPI

REMISE DES PIÈCES DATE 24 JUIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0309086
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 24 JUIL. 2003

Vos références pour ce dossier *(facultatif)* BdR/BR 61423

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

NOVAGRAAF TECHNOLOGIES
122, rue Edouard Vaillant
92593 Levallois Perret Cedex
FRANCE

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et système de double authentification sécurisée d'un utilisateur lors de l'accès à un service par l'intermédiaire d'un réseau IP

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation Date N°
Pays ou organisation Date N°
Pays ou organisation Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases)		☒ Personne morale ☐ Personne physique
Nom ou dénomination sociale		FRANCE TELECOM
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	6, place d'Alleray
	Code postal et ville	7 5 0 1 5 Paris
	Pays	FRANCE
Nationalité		FRANCAISE
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 24 JUIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0309086

DB 540 @ W / 010801

Vos références pour ce dossier : *(facultatif)*		BdR/BR 61423
6 MANDATAIRE *(s'il y a lieu)*		
Nom		DE ROQUEMAUREL
Prénom		Bruno
Cabinet ou Société		NOVAGRAAF TECHNOLOGIES
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	122, rue Edouard Vaillant
	Code postal et ville	9 2 5 9 3 Levallois Perret Cedex
	Pays	FRANCE
N° de téléphone *(facultatif)*		01 49 64 61 00
N° de télécopie *(facultatif)*		01 49 64 61 30
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'Inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : AG
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
DE ROQUEMAUREL Bruno 02-0407

VISA DE LA PRÉFECTURE OU DE L'INPI

P. COINTE

PROCEDE ET SYSTEME DE DOUBLE AUTHENTIFICATION SECURISEE D'UN UTILISATEUR LORS DE L'ACCES A UN SERVICE PAR L'INTERMEDIAIRE D'UN RESEAU IP.

La présente invention concerne la fourniture de services basés sur un transport IP (Internet Protocol), tels que les services accessibles par l'intermédiaire du réseau Internet ou des services conversationnels sur IP.

A l'heure actuelle, lorsqu'un utilisateur souhaite accéder à un tel service, il doit se connecter au réseau IP par l'intermédiaire d'un réseau d'accès et d'un fournisseur de service (FS) tel qu'un fournisseur d'accès Internet. A cet effet, il doit préalablement être authentifié par un serveur d'authentification du fournisseur de service. Pour cela, il doit lui transmettre un identifiant de la forme identifiantFS@domaineFS et un mot de passe. Une telle authentification permet au fournisseur de service de personnaliser ses services, par exemple en transmettant à l'utilisateur une page d'accueil dans laquelle figure le nom de l'utilisateur.

Une fois que l'utilisateur est connecté au réseau Internet, il peut accéder à d'autres services qui peuvent également proposer une identification et authentification de l'utilisateur afin de pouvoir lui offrir des services à forte valeur ajoutée. Par exemple, un service de banque en ligne sur Internet nécessite un opérateur de réseau d'accès, un fournisseur d'accès à Internet et la banque concernée. Un accès à un réseau Intranet d'entreprise nécessite au moins un opérateur de réseau d'accès et l'entreprise concernée.

Plusieurs authentifications peuvent donc être effectuées durant une même connexion. Comme ces authentifications sont réalisées par des acteurs différents du réseau, elles sont effectuées d'une manière indépendante, ce qui oblige l'utilisateur à exécuter plusieurs procédures d'authentification. L'ergonomie ainsi offerte à l'utilisateur apparaît donc médiocre, et fastidieuse.

Par ailleurs, il s'avère que les procédures d'authentification utilisées actuellement par les fournisseurs de services et qui sont basées sur la fourniture d'un identifiant et d'un mot de passe, offrent une sécurité médiocre, et en tout cas, insuffisante pour permettre à un acteur de jouer le rôle de tiers de confiance vis-à-vis d'autres fournisseurs de services.

Dans le cas de réseaux d'accès, les procédures d'authentification actuelles qui sont exécutées durant les connexions IP/PPP (Point-to-Point Protocol) via un réseau RTC (Réseau Téléphonique Commuté), RNIS (Réseau Numérique à Intégration de Services) ou l'ADSL (Asymmetric Digital Subscriber Line), ne permettent pas d'effectuer une authentification au niveau du réseau d'accès pour les connexion PPP. Généralement, l'opérateur de réseau ORA/OTI (Opérateur de Réseaux d'Accès / de Transport IP) ne peut pas utiliser les informations transmises par l'utilisateur pour être authentifié auprès du fournisseur de service, dans le but d'identifier l'utilisateur, car il ne maîtrise pas ces informations qui sont gérées par un autre domaine administratif.

Il existe par ailleurs une procédure d'authentification sécurisée basée sur un mécanisme de défi / réponse (Challenge / Response) qui a été normalisée par exemple par le protocole CHAP (Challenge Handshake Authentication Protocol). Toutefois, cette procédure est conçue pour effectuer une authentification sécurisée vis-à-vis d'un seul acteur indépendant, et doit donc être exécutée à nouveau pour chaque acteur auprès duquel une authentification est souhaitée.

La présente invention a pour but de supprimer ces inconvénients en proposant un procédé permettant d'effectuer une authentification pour plusieurs acteurs indépendants du réseau. Cet objectif est atteint par la prévision d'un procédé d'authentification d'un utilisateur lors d'une tentative d'accès à un acteur d'un réseau de transport IP, ce procédé comprenant des étapes au cours desquelles :

- un terminal d'utilisateur émet à un acteur du réseau une requête d'accès contenant des données d'identification et d'authentification de l'utilisateur auprès de l'acteur, la requête d'accès étant transmise par l'intermédiaire d'un réseau d'accès et d'un réseau de transport IP à un serveur d'authentification de l'acteur,
- le serveur d'authentification exécute une procédure d'authentification de l'utilisateur sur la base des données d'identification et d'authentification contenues dans la requête d'accès, et
- le serveur d'authentification transmet au terminal d'utilisateur un message de réponse contenant le résultat de l'authentification de l'utilisateur par le serveur d'authentification.

Selon l'invention, ce procédé comprend en outre des étapes au cours desquelles :

- un nombre aléatoire est transmis au terminal préalablement à l'émission de la requête d'accès,
- des données d'authentification de l'utilisateur auprès d'au moins deux acteurs du réseau sont calculées à l'aide d'au moins un algorithme cryptographique prédéfini et d'au moins une clé secrète propre à l'utilisateur,
- le terminal insère dans la requête d'accès des données d'identification de l'utilisateur auprès desdits acteurs du réseau et les données d'authentification calculées, et
- le terminal transmet la requête d'accès à un contrôleur d'accès qui transmet à chacun des deux acteurs une requête d'authentification respective contenant respectivement les données d'identification et d'authentification de l'utilisateur auprès desdits acteurs du réseau, contenues dans la requête d'accès,
- des serveurs d'authentification de chacun des acteurs exécutent une procédure d'authentification de l'utilisateur, sur la base des données d'identification et d'authentification de l'utilisateur, contenues dans les requêtes d'authentification, et
- des comptes rendus d'authentification contenant des résultats des procédures d'authentification exécutées par les serveurs d'authentification de chacun desdits acteurs du réseau sont transmises au terminal.

Avantageusement, au moins l'une des données d'authentification est calculée par un module connecté au terminal.

Selon un mode de réalisation de l'invention, ce procédé comprend une étape préalable au cours de laquelle le terminal établit une connexion avec un serveur spécialisé par l'intermédiaire du réseau, le nombre aléatoire étant généré et transmis au terminal par le serveur spécialisé à la suite de l'établissement de la connexion.

Selon un autre mode de réalisation de l'invention, la requête d'accès émise par le terminal est transmise au serveur spécialisé qui y insère le nombre aléatoire utilisé pour calculer les données d'authentification, la requête d'accès étant ensuite transmise au contrôleur d'accès qui insère le nombre aléatoire dans les requêtes d'authentification transmises aux deux acteurs.

Selon encore un autre mode de réalisation de l'invention, les procédures d'authentification exécutées par les serveurs d'authentification des acteurs comprennent une étape de recherche de la clé secrète de l'utilisateur sur la base de la donnée d'identification contenue dans la requête d'authentification, une étape de calcul d'une donnée d'authentification en exécutant l'algorithme cryptographique avec la clé secrète de l'utilisateur et le nombre aléatoire contenu dans la requête d'authentification, et une étape de comparaison de la donnée d'authentification contenue dans la requête d'authentification, avec la donnée d'authentification calculée, l'utilisateur étant correctement authentifié si la donnée d'authentification contenue dans la requête d'authentification correspond à la donnée d'authentification calculée.

Selon encore un autre mode de réalisation de l'invention, les acteurs du réseau comprennent plusieurs acteurs parmi des fournisseurs d'accès offrant à l'utilisateur un accès au réseau Internet, des fournisseurs de service IP, et un opérateur de réseau d'accès et de transport IP.

Avantageusement, les données d'identification insérées dans la requête d'accès sont de la forme :

"IdA@DomaineA"

dans laquelle :

- "IdA" représente l'identifiant de l'utilisateur auprès de l'acteur du réseau,
- "DomaineA" représente l'identifiant de l'acteur du réseau dans le réseau de transport IP,

le contrôleur d'accès déterminant les acteurs vers lesquels transmettre les requêtes d'authentification sur la base des identifiants "DomaineA" de l'acteur du réseau contenus dans la requête d'accès.

Avantageusement, les étapes d'authentification de l'utilisateur par les serveurs d'authentification des acteurs sont effectuées l'une à la suite de l'autre.

Alternativement, les étapes d'authentification de l'utilisateur par les serveurs d'authentification des acteurs sont déclenchées sensiblement simultanément.

De préférence, le nombre aléatoire à partir duquel les données

tentative de connexion.

Selon encore un autre mode de réalisation de l'invention, les procédures d'authentification de l'utilisateur sont effectuées conformément au protocole CHAP.

L'invention concerne également un système d'authentification d'un utilisateur lors d'une tentative d'accès à un acteur d'un réseau de transport IP auquel sont connectés des acteurs du réseau, et auquel des terminaux d'utilisateurs peuvent accéder par l'intermédiaire de réseaux d'accès, ce système comprenant :

- des moyens prévus dans chaque terminal d'utilisateur pour émettre des requêtes d'accès à un acteur du réseau, ces requêtes contenant des données d'identification et d'authentification de l'utilisateur auprès de l'acteur du réseau, et
- au moins un serveur d'authentification pour chacun des acteurs du réseau, conçu pour identifier et authentifier les utilisateurs en fonction des données d'identification et d'authentification contenues dans les requêtes d'accès reçues.

Selon l'invention, chaque terminal d'utilisateur comprend des moyens pour recevoir un nombre aléatoire lors de l'établissement d'une connexion avec le réseau de transport IP, des moyens de calculs cryptographiques pour appliquer au moins un algorithme cryptographique prédéfini au nombre aléatoire reçu afin d'obtenir des données d'authentification de l'utilisateur auprès d'au moins deux acteurs du réseau, et des moyens pour insérer dans chaque requête d'accès émise des données d'identification de l'utilisateur auprès des deux acteurs du réseau et les données d'authentification calculées, le système comportant en outre un contrôleur d'accès comprenant des moyens pour recevoir les requêtes d'accès provenant des terminaux d'utilisateurs et transmises par le réseau de transport IP, des moyens pour extraire de chacune des requêtes d'accès les données d'identification et d'authentification de l'utilisateur auprès d'au moins deux acteurs du réseau, des moyens pour transmettre à chacun des deux acteurs une requête d'authentification respective contenant respectivement les données d'identification et d'authentification de l'utilisateur auprès des deux acteurs, contenues dans la requête d'accès.

Selon un mode de réalisation de l'invention, ce système comprend un module externe conçu pour se connecter à chacun des terminaux d'utilisateurs et comprenant des moyens pour recevoir le nombre aléatoire du terminal auquel il est connecté, des moyens de calcul cryptographique pour exécuter l'algorithme cryptographique prédéfini sur la base du nombre aléatoire, et pour transmettre au terminal au moins une donnée d'authentification de l'utilisateur auprès d'un acteur du réseau obtenue par les calculs cryptographiques.

Avantageusement, l'algorithme prédéfini est un algorithme cryptographique utilisant une clé secrète propre à l'utilisateur et mémorisée par le module.

Selon un autre mode de réalisation de l'invention, le module est une carte à microprocesseur, chaque terminal comportant des moyens pour se connecter à une carte à microprocesseur.

Selon un autre mode de réalisation de l'invention, le contrôleur d'accès comprend en outre des moyens pour recevoir des comptes rendus d'authentification de l'utilisateur, émis par les acteurs en réponse aux requêtes d'authentification, et des moyens pour transmettre au terminal d'utilisateur un compte rendu d'authentification sur la base des comptes rendus reçus des acteurs.

Selon encore un autre mode de réalisation de l'invention, ce système comprend en outre un serveur spécialisé connecté au réseau de manière à être connecté aux terminaux d'utilisateurs à la suite de l'établissement d'une connexion du terminal au réseau, le serveur spécialisé comprenant des moyens pour générer et transmettre un nombre aléatoire à chacun des terminaux avec lesquels une connexion est établie, et des moyens pour insérer le nombre aléatoire dans chacune des requêtes d'accès émises par les terminaux.

De préférence, le serveur spécialisé est un serveur HTTP comportant une interface avec le protocole RADIUS.

Egalement de préférence, le contrôleur d'accès est un Proxy RADIUS.

Selon encore un autre mode de réalisation de l'invention, chaque acteur du réseau comprend des moyens de stockage de clés secrètes d'utilisateurs, des

l'acteur en appliquant au nombre aléatoire reçu dans une requête d'authentification et à la clé secrète d'un utilisateur l'algorithme prédéfini, et pour comparer le résultat obtenu à la donnée d'authentification de l'utilisateur reçue dans la requête d'authentification, l'utilisateur étant correctement authentifié par l'acteur uniquement si le résultat du calcul cryptographique obtenu est égal à la donnée d'authentification contenue dans la requête d'authentification.

Un mode de réalisation préféré de l'invention sera décrit ci-après, à titre d'exemple non limitatif, avec référence aux dessins annexés dans lesquels :

La figure 1 représente schématiquement l'architecture d'un système de fourniture de services basés sur un transport IP, selon l'invention ;

La figure 2 représente un diagramme de séquencement d'étapes qui sont exécutées dans le système représenté sur la figure 1, conformément au procédé selon l'invention.

Le système représenté sur la figure 1 comprend des réseaux d'accès 1, 2 auxquels sont connectés des terminaux 11 d'utilisateurs. Ces réseaux d'accès 1, 2 fournissent aux terminaux 11 un accès à un réseau de transport IP 5 par l'intermédiaire de passerelles IP 3, 4 respectives adaptées au réseau d'accès. L'ensemble des réseaux d'accès, des passerelles et du réseau de transport IP est mis en œuvre par un opérateur ORA/OTI de réseaux d'accès et de transport IP.

Le réseau de transport IP 5 permet aux utilisateurs d'accéder à un fournisseur d'accès Internet 6, 7 ou à un fournisseur de services IP 8.

A cet effet, ce système comprend, selon l'invention, un serveur spécialisé 12 qui délivre aux utilisateurs souhaitant se connecter au réseau IP, des nombres aléatoires destinés à être utilisés au cours de procédures d'identification, et un contrôleur d'accès 10 connecté au réseau de transport IP 5 et auquel le serveur spécialisé 12 transmet les requêtes d'accès émises par les terminaux 11.

Le contrôleur d'accès 10 est conçu pour recevoir toutes les requêtes d'accès à un fournisseur 6, 7, 8 d'accès ou de service, émises par les utilisateurs sur les réseaux 1, 2, par l'intermédiaire de la passerelle 3, 4 correspondant au réseau

d'accès 1, 2 employé, et du serveur spécialisé 12, et d'aiguiller ces requêtes au travers du réseau de transport IP vers le fournisseur 6, 7, 8 d'accès ou de service indiqué dans la requête par le terminal de l'utilisateur.

Il est à noter que les passerelles 3, 4 peuvent alternativement assurer les fonctions exécutées par le serveur spécialisé 12.

Pour accéder au réseau IP 5 par l'intermédiaire d'un fournisseur d'accès 6, 7 et à un service particulier offert par un fournisseur de service 8 connecté au réseau, le terminal de l'utilisateur exécute tout d'abord une procédure d'établissement de connexion avec le serveur spécialisé 12 pour obtenir un nombre aléatoire RAND. Ensuite, le terminal de l'utilisateur émet une requête d'accès au fournisseur de service souhaité via le fournisseur d'accès, qui est transmise successivement par la passerelle IP 3, 4 et par le serveur spécialisé 12 au contrôleur d'accès 10. A la réception d'une telle requête, le contrôleur d'accès 10 demande au fournisseur d'accès 6, 7 et au fournisseur de service 8 demandés d'authentifier l'utilisateur. Lorsque le fournisseur d'accès et le fournisseur de service ont envoyé leur réponse concernant l'authentification de l'utilisateur, le contrôleur d'accès émet une réponse d'autorisation d'accès à destination du terminal 11 de l'utilisateur, en fonction des réponses d'authentification reçues.

Le séquencement des étapes du procédé d'authentification selon l'invention est illustré par le diagramme représenté sur la figure 2.

Pour accéder à un service IP, le terminal 11 de l'utilisateur exécute tout d'abord une procédure 21 d'établissement d'une connexion avec le serveur spécialisé 12 via une passerelle IP 3, 4 accessible au terminal, l'adresse du serveur spécialisé étant par exemple connue du logiciel de connexion installé dans le terminal. Cette procédure consiste tout d'abord à établir une connexion avec la passerelle IP 3, 4, par exemple conformément au protocole LCP (Link Control Protocol). Juste après l'ouverture de la connexion, un nombre aléatoire RAND est envoyé par le serveur spécialisé 12 au terminal 11 (étape 22), par exemple sous la forme d'un message de défi 41 conforme au protocole CHAP.

Ce nombre aléatoire est destiné à servir de base à des calculs de mots de passe utilisables uniquement pour la tentative de connexion et d'accès en cours. Ces

cryptographie faisant intervenir une ou plusieurs clés secrètes et le nombre aléatoire RAND fourni par le serveur spécialisé pour la connexion en cours. Les algorithmes cryptographiques peuvent être mis en œuvre par le terminal de l'utilisateur, et/ou de préférence par un module 15 physiquement indépendant de ce dernier, par exemple de type carte à microprocesseur.

Dans ce dernier cas, le logiciel de connexion installé dans le terminal est en outre conçu pour interroger le module 15.

L'algorithme de cryptographie choisi est par exemple celui qui est implémenté dans les cartes SIM (Subscriber Identification Module) des terminaux mobiles de type GSM (Global System for Mobile communications).

A la réception du message de défi 41, le terminal en extrait le nombre aléatoire RAND 42 et le transmet au module 15 connecté au terminal (étape 23).

A l'étape suivante 24, le module 15 applique un algorithme de cryptographie au nombre aléatoire reçu en utilisant une clé secrète de l'utilisateur, ce qui permet d'obtenir un nombre 43 à utiliser comme mot de passe d'authentification de l'utilisateur. Pour accéder à plusieurs acteurs du réseau choisis par l'utilisateur, à savoir par exemple un fournisseur d'accès et un fournisseur de service, autant de mots de passe que d'acteurs à accéder sont de préférence générés par le terminal et/ou par le module 15, avec le même algorithme cryptographique ou avec des algorithmes différents, et avec la même clé secrète ou avec des clés secrètes différentes. Les mots de passe AUTH1, AUTH2 éventuellement calculés par le module 15 sont ensuite transmis en réponse au terminal 11.

Bien entendu, si l'un ou les deux algorithmes cryptographiques sont installés dans le terminal, l'étape 24 est au moins partiellement exécutée par le terminal.

Une fois la connexion avec le serveur spécialisé 12 établie, le terminal envoie un message 44 de requête d'accès à celui-ci (étape 25). Ce message de requête 44 comprend les identifiants ID1 et ID2 de l'utilisateur respectivement auprès du fournisseur d'accès et du service choisi, et les mots de passe AUTH1 et AUTH2 obtenus par les calculs cryptographiques.

A la réception du message de requête 44, le serveur spécialisé 12 encapsule ce message dans une requête d'autorisation d'accès 45 (étape 26). Cette requête est

par exemple du type "Access-Request" conforme au protocole RADIUS (Remote Authentication Dial In User Service) comportant un attribut nom d'utilisateur "User-Name" égal aux deux identifiants concaténés ID1|ID2, un attribut mot de passe "CHAP-Password" égal aux deux mots de passe concaténés AUTH1|AUTH2, ainsi qu'un attribut "CHAP-Challenge" destiné à recevoir le nombre aléatoire RAND utilisé pour générer les mots de passe, le nombre RAND étant déterminé par le serveur spécialisé en fonction d'un identifiant de la session de connexion en cours avec le terminal. La requête 45 est transmise par le serveur spécialisé 12 au contrôleur d'accès 10.

A l'étape 27 suivante, le contrôleur d'accès reçoit la requête 45 et en extrait les paramètres d'identification et d'authentification. Ces paramètres sont transmis aux étapes 28, 29 dans des messages d'authentification 46, 47 respectivement aux serveurs d'authentification 16 du fournisseur d'accès et du fournisseur de service choisi. Les informations d'identification ID1 et ID2 sont par exemple de la forme "IdA@domaineA", "IdA" permettant d'identifier d'une manière unique l'utilisateur auprès du fournisseur d'accès ou de service, et "domaineA" permettant de déterminer le nom de domaine dans le réseau IP, du serveur vers lequel doit être envoyé le message d'authentification correspondant. Ces messages d'authentification 46, 47 contiennent chacun l'identifiant et le mot de passe correspondant au destinataire du message, ainsi que le nombre aléatoire RAND.

A la réception d'un tel message d'authentification 46, 47, le serveur d'authentification 16 exécute une procédure d'authentification 28, respectivement 29. Cette procédure d'authentification consiste à identifier l'utilisateur grâce à l'information d'identification ID1, respectivement ID 2, puis à déterminer la clé secrète de l'utilisateur en accédant à une base de données de clés secrètes d'utilisateurs autorisés, à calculer ensuite le mot de passe de l'utilisateur à l'aide de cette clé secrète et du nombre RAND reçu, et enfin à comparer le mot de passe ainsi calculée avec celui qui a été reçu. Pour calculer le mot de passe AUTH, le serveur d'authentification dispose du même algorithme cryptographique que celui utilisé par le terminal 11 ou le module 15.

L'utilisateur est correctement authentifié uniquement si le mot de passe calculé par le serveur d'authentification est identique à celui qui a été reçu.

contrôleur d'accès 10 sous la forme d'un message 48, respectivement 49 de compte-rendu d'authentification.

A la réception des deux messages 48, 49 de compte-rendu d'authentification, en provenance respectivement du fournisseur d'accès 6, 7 et du fournisseur de service IP 8 choisi, le contrôleur d'accès 10 dispose des informations nécessaires pour gérer les droits d'accès de l'utilisateur en fonction de la politique de l'opérateur ORA/OTI et exécute une étape 30 de génération d'un message 50 de réponse à la requête d'accès émise par l'utilisateur et transmet ce message de réponse au serveur spécialisé 12.

Ce message de réponse 50 contient les comptes-rendus d'authentification émis par le fournisseur d'accès 6, 7, et par le fournisseur de service 8 choisi.

Il est à noter que les procédures d'authentification 28 et 29 exécutées par le fournisseur d'accès 6, 7 et le fournisseur de service 8 peuvent être exécutées simultanément ou bien séquentiellement dans un ordre quelconque.

A la réception du message de réponse 50, le serveur spécialisé 12 exécute une procédure 31 consistant à extraire de ce message de réponse les informations à renvoyer à l'utilisateur, puis à transmettre au terminal d'utilisateur dans un message 51, par exemple de type "CHAP-success" ou "Chap-failure" pour le protocole CHAP, les informations extraites qui lui sont destinées.

Grâce à ces dispositions, un utilisateur peut être authentifié simultanément par différents acteurs du réseau, par exemple bénéficier d'un accès à Internet dans lequel il a été authentifié par un service de paiement en ligne sécurisé, par exemple offert par un organisme bancaire. Il peut en outre être authentifié par l'opérateur ORA/OTI.

L'invention qui vient d'être décrite peut être réalisée en mettant en œuvre un serveur spécialisé 12 du type serveur HTTP, et un contrôleur d'accès 10 du type proxy RADIUS, le serveur spécialisé comportant une interface RADIUS pour pouvoir communiquer avec le contrôleur d'accès, les serveurs d'authentification étant également des serveurs RADIUS.

REVENDICATIONS

1. Procédé d'authentification d'un utilisateur lors d'une tentative d'accès à un acteur (6, 7, 8) d'un réseau de transport IP (5), ce procédé comprenant des étapes au cours desquelles :

- un terminal (11) d'utilisateur émet à un acteur du réseau (5) une requête d'accès (44) contenant des données d'identification et d'authentification de l'utilisateur auprès de l'acteur, la requête d'accès étant transmise par l'intermédiaire d'un réseau d'accès (1, 2) et d'un réseau de transport IP (5) à un serveur d'authentification (16) de l'acteur,
- le serveur d'authentification exécute une procédure d'authentification (28) de l'utilisateur sur la base des données d'identification et d'authentification contenues dans la requête d'accès, et
- le serveur d'authentification (16) transmet au terminal (11) d'utilisateur un message de réponse (51) contenant le résultat de l'authentification de l'utilisateur par le serveur d'authentification (16),

caractérisé en ce qu'il comprend en outre des étapes au cours desquelles :

- un nombre aléatoire est transmis au terminal (11) préalablement à l'émission de la requête d'accès (44),
- des données d'authentification de l'utilisateur auprès d'au moins deux acteurs (6, 7, 8) du réseau (5) sont calculées à l'aide d'au moins un algorithme cryptographique prédéfini et d'au moins une clé secrète propre à l'utilisateur,
- le terminal (11) insère dans la requête d'accès (44) des données d'identification de l'utilisateur auprès desdits acteurs du réseau (5) et les données d'authentification calculées, et
- le terminal (11) transmet la requête d'accès à un contrôleur d'accès (10) qui transmet à chacun des deux acteurs une requête d'authentification (46, 47) respective contenant respectivement les données d'identification et d'authentification de l'utilisateur auprès desdits acteurs du réseau (5), contenues dans la requête d'accès,
- des serveurs d'authentification (16) de chacun des acteurs exécutent une procédure d'authentification (28, 29) de l'utilisateur, sur la base des données d'identification et d'authentification de l'utilisateur, contenues dans les requêtes d'authentification (46, 47), et
- des comptes rendus d'authentification contenant des résultats des procédures d'authentification exécutées par les serveurs d'authentification (16) de

2. Procédé selon la revendication 1,
caractérisé en ce qu'au moins l'une des données d'authentification est calculée par un module (15) connecté au terminal (11).

3. Procédé selon la revendication 1 ou 2,
caractérisé en ce qu'il comprend une étape préalable au cours de laquelle le terminal établit une connexion avec un serveur spécialisé (12) par l'intermédiaire du réseau (5), le nombre aléatoire étant généré et transmis au terminal (11) par le serveur spécialisé à la suite de l'établissement de la connexion.

4. Procédé selon la revendication 3,
caractérisé en ce que la requête d'accès (44) émise par le terminal est transmise au serveur spécialisé (12) qui y insère le nombre aléatoire utilisé pour calculer les données d'authentification, la requête d'accès étant ensuite transmise au contrôleur d'accès (10) qui insère le nombre aléatoire dans les requêtes d'authentification transmises aux deux acteurs (6, 7, 8).

5. Procédé selon la revendication 4,
caractérisé en ce que les procédures d'authentification exécutées par les serveurs d'authentification (16) des acteurs (6, 7, 8) comprennent une étape de recherche de la clé secrète de l'utilisateur sur la base de la donnée d'identification contenue dans la requête d'authentification, une étape de calcul d'une donnée d'authentification en exécutant l'algorithme cryptographique avec la clé secrète de l'utilisateur et le nombre aléatoire contenu dans la requête d'authentification, et une étape de comparaison de la donnée d'authentification contenue dans la requête d'authentification, avec la donnée d'authentification calculée, l'utilisateur étant correctement authentifié si la donnée d'authentification contenue dans la requête d'authentification correspond à la donnée d'authentification calculée.

6. Procédé selon l'une des revendications 1 à 5,
caractérisé en ce que les acteurs (6, 7, 8) du réseau (5) comprennent plusieurs acteurs parmi des fournisseurs d'accès (6, 7) offrant à l'utilisateur un accès au réseau Internet, des fournisseurs de service (8) IP, et un opérateur de réseau d'accès et de transport IP.

7. Procédé selon l'une des revendications 1 à 6,
caractérisé en ce que les données d'identification insérées dans la requête d'accès (44) sont de la forme :

"IdA@DomaineA"

dans laquelle :
- "IdA" représente l'identifiant de l'utilisateur auprès de l'acteur du réseau,
- "DomaineA" représente l'identifiant de l'acteur du réseau dans le réseau de transport IP (5),

le contrôleur d'accès (10) déterminant les acteurs vers lesquels transmettre les requêtes d'authentification (46, 47) sur la base des identifiants "DomaineA" de l'acteur du réseau contenus dans la requête d'accès (44).

8. Procédé selon l'une des revendications 1 à 7,
caractérisé en ce que les étapes d'authentification (28, 29) de l'utilisateur par les serveurs d'authentification (16) des deux acteurs (6, 7, 8) sont effectuées l'une à la suite de l'autre.

9. Procédé selon l'une des revendications 1 à 7,
caractérisé en ce que les étapes d'authentification (28, 29) de l'utilisateur par les serveurs d'authentification (16) des deux acteurs (6, 7, 8) sont déclenchées sensiblement simultanément.

10. Procédé selon l'une des revendications 1 à 9,
caractérisé en ce que le nombre aléatoire à partir duquel les données d'authentification sont calculées est un nombre aléatoire modifié à chaque tentative de connexion.

11. Procédé selon l'une des revendications 1 à 10,
caractérisé en ce que les procédures d'authentification de l'utilisateur sont effectuées conformément au protocole CHAP.

12. Système d'authentification d'un utilisateur lors d'une tentative d'accès à un acteur (6, 7, 8) d'un réseau de transport IP (5) auquel sont connectés des acteurs du réseau, et auquel des terminaux d'utilisateurs peuvent accéder par l'intermédiaire de réseaux d'accès (1, 2), ce système comprenant :
- des moyens prévus dans chaque terminal d'utilisateur pour émettre des [illegible]

données d'identification et d'authentification de l'utilisateur auprès de l'acteur du réseau, et

- au moins un serveur d'authentification (16) pour chacun des acteurs du réseau, conçu pour identifier et authentifier les utilisateurs en fonction des données d'identification et d'authentification contenues dans les requêtes d'accès reçues,

caractérisé en ce que chaque terminal (11) d'utilisateur comprend des moyens pour recevoir un nombre aléatoire lors de l'établissement d'une connexion avec le réseau de transport IP (5), des moyens de calculs cryptographiques pour appliquer au moins un algorithme cryptographique prédéfini au nombre aléatoire reçu afin d'obtenir des données d'authentification de l'utilisateur auprès d'au moins deux acteurs du réseau (5), et des moyens pour insérer dans chaque requête d'accès (44) émise des données d'identification de l'utilisateur auprès des deux acteurs du réseau et les données d'authentification calculées, le système comportant en outre un contrôleur d'accès (10) comprenant des moyens pour recevoir les requêtes d'accès provenant des terminaux d'utilisateurs et transmises par le réseau de transport IP (5), des moyens pour extraire de chacune des requêtes d'accès les données d'identification et d'authentification de l'utilisateur auprès d'au moins deux acteurs du réseau, des moyens pour transmettre à chacun des deux acteurs une requête d'authentification (46, 47) respective contenant respectivement les données d'identification et d'authentification de l'utilisateur auprès des deux acteurs, contenues dans la requête d'accès (44).

13. Système selon la revendication 12,

caractérisé en ce qu'il comprend un module externe (15) conçu pour se connecter à chacun des terminaux (11) d'utilisateurs et comprenant des moyens pour recevoir le nombre aléatoire du terminal auquel il est connecté, des moyens de calcul cryptographique pour exécuter l'algorithme cryptographique prédéfini sur la base du nombre aléatoire, et pour transmettre au terminal au moins une donnée d'authentification de l'utilisateur auprès d'un acteur (6, 7, 8) du réseau (5) obtenue par les calculs cryptographiques.

14. Système selon la revendication 13,

caractérisé en ce que l'algorithme prédéfini est un algorithme cryptographique utilisant une clé secrète propre à l'utilisateur et mémorisée par le module (15).

15. Système selon la revendication 13 ou 14,

caractérisé en ce que le module (15) est une carte à microprocesseur, chaque terminal (11) comportant des moyens pour se connecter à une carte à microprocesseur.

16. Système selon l'une des revendications 12 à 15, caractérisé en ce que le contrôleur d'accès (10) comprend en outre des moyens pour recevoir des comptes rendus d'authentification (48, 49) de l'utilisateur, émis par les acteurs en réponse aux requêtes d'authentification, et des moyens pour transmettre au terminal d'utilisateur un compte rendu d'authentification (51) sur la base des comptes rendus reçus des acteurs.

17. Système selon l'une des revendications 12 à 16, caractérisé en ce qu'il comprend en outre un serveur spécialisé (12) connecté au réseau (5) de manière à être connecté aux terminaux (11) d'utilisateurs à la suite de l'établissement d'une connexion du terminal au réseau, le serveur spécialisé comprenant des moyens pour générer et transmettre un nombre aléatoire à chacun des terminaux avec lesquels une connexion est établie, et des moyens pour insérer le nombre aléatoire dans chacune des requêtes d'accès émises par les terminaux.

18. Système selon la revendication 17, caractérisé en ce que le serveur spécialisé (12) est un serveur HTTP comportant une interface avec le protocole RADIUS.

19. Système selon l'une des revendications 12 à 18, caractérisé en ce que le contrôleur d'accès (10) est un Proxy RADIUS.

20. Système selon l'une des revendications 12 à 19, caractérisé en ce que chaque acteur (6, 7, 8) du réseau (5) comprend des moyens de stockage de clés secrètes d'utilisateurs, des moyens pour déterminer la donnée d'authentification de l'utilisateur auprès de l'acteur en appliquant au nombre aléatoire reçu dans une requête d'authentification (46, 47) et à la clé secrète d'un utilisateur l'algorithme prédéfini, et pour comparer le résultat obtenu à la donnée d'authentification de l'utilisateur reçue dans la requête d'authentification, l'utilisateur étant correctement authentifié par l'acteur uniquement si le résultat du calcul cryptographique obtenu est égal à la donnée d'authentification contenue dans la requête d'authentification.

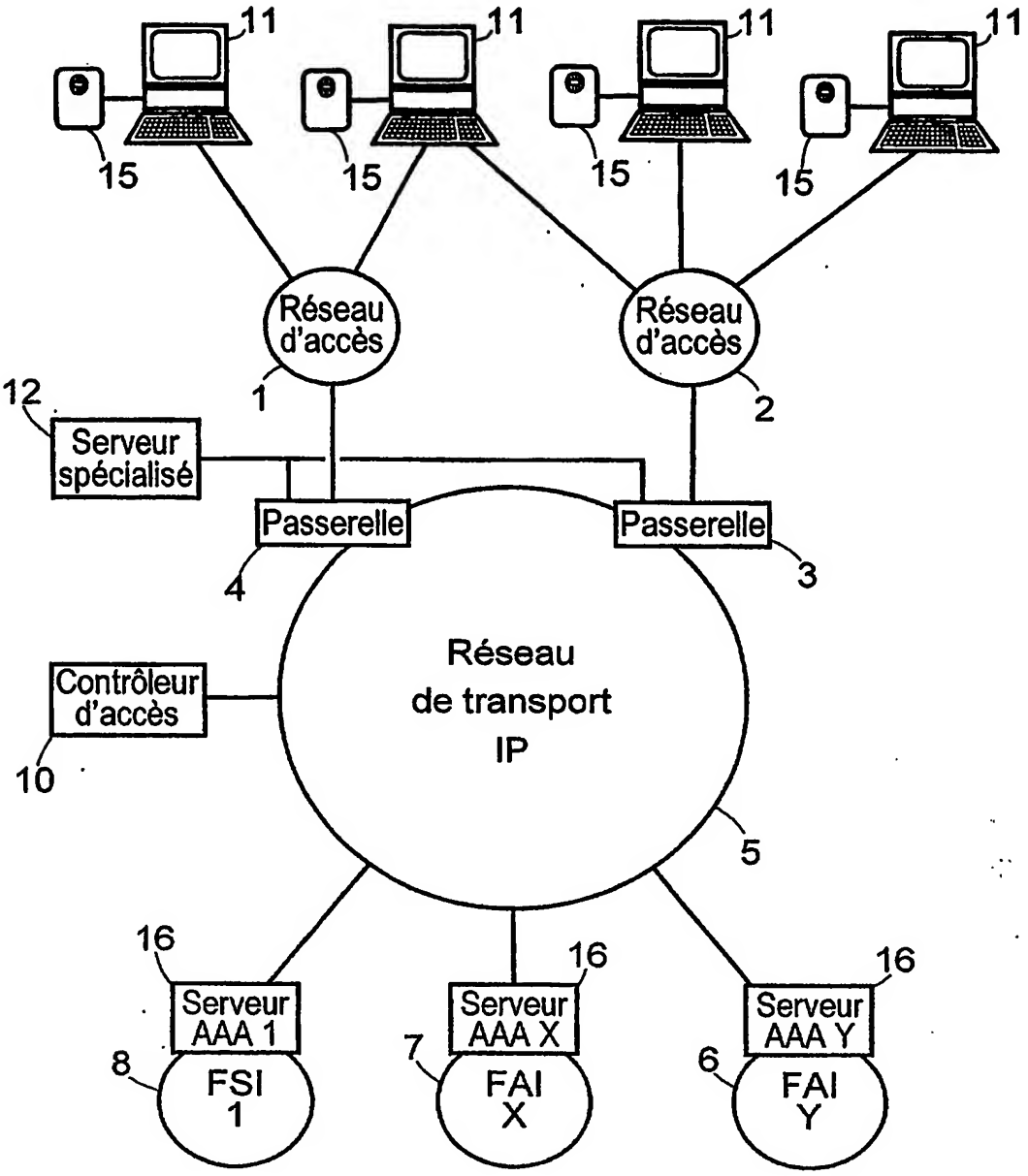
11
11
11
11
15
15
15
15
Réseau d'accès
Réseau d'accès
1
2
12
Serveur spécialisé
Passerelle
Passerelle
4
3
Réseau de transport IP
Contrôleur d'accès
10
5
16
16
16
Serveur AAA 1
Serveur AAA X
Serveur AAA Y
8
7
6
FSI 1
FAI X
FAI Y

Fig. 1

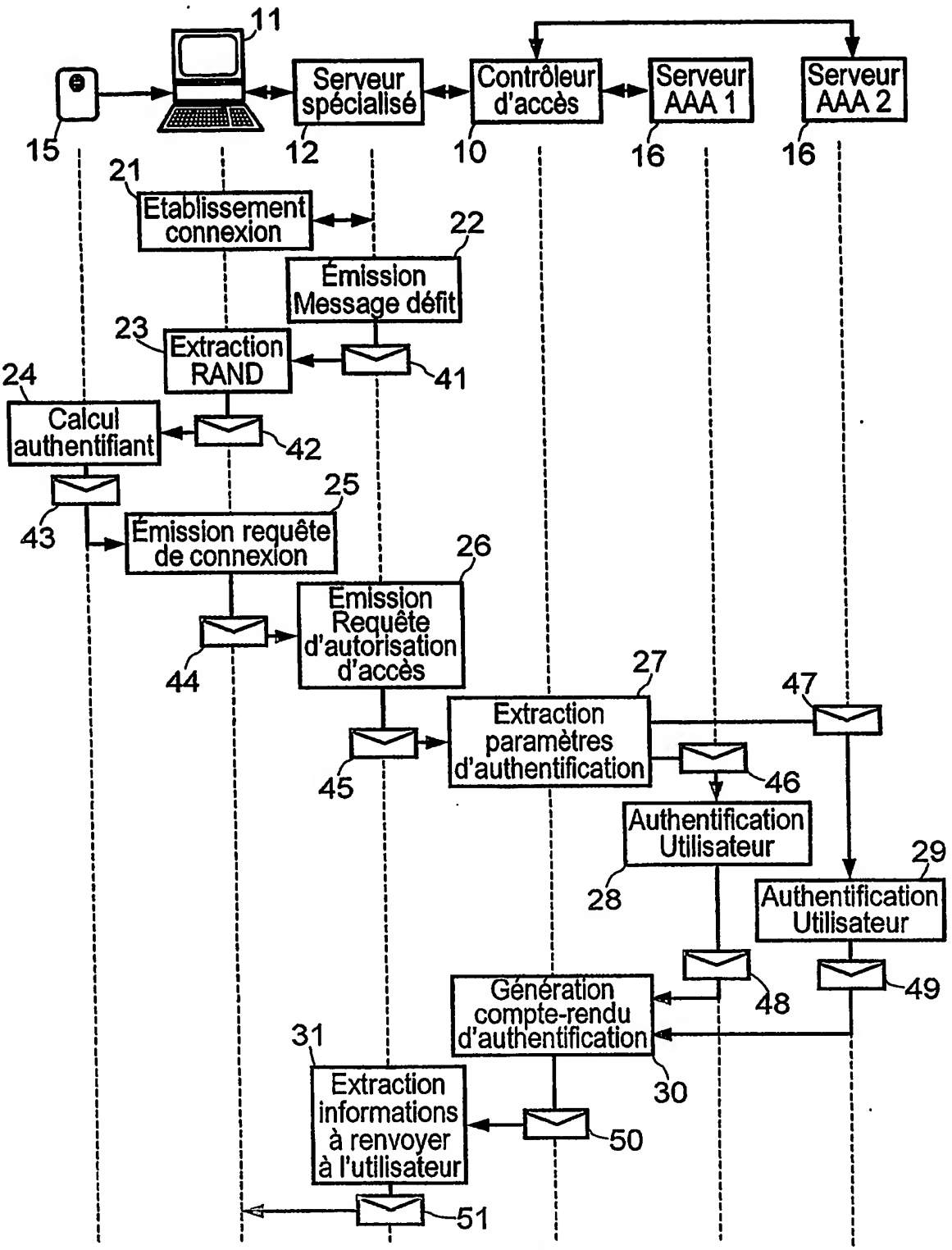
11
15
Serveur spécialisé
12
Contrôleur d'accès
10
Serveur AAA 1
16
Serveur AAA 2
16
21
Etablissement connexion
22
Émission Message défit
23
Extraction RAND
41
24
Calcul authentifiant
42
43
25
Émission requête de connexion
26
Émission Requête d'autorisation d'accès
44
27
Extraction paramètres d'authentification
45
47
46
Authentification Utilisateur
28
29
Authentification Utilisateur
48
49
Génération compte-rendu d'authentification
30
31
Extraction informations à renvoyer à l'utilisateur
50
51

Fig. 2

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire — DB 113 W /260699

Vos références pour ce dossier *(facultatif)*	BdR/BR 61423
N° D'ENREGISTREMENT NATIONAL	0309086

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
Procédé et système de double authentification sécurisée d'un utilisateur lors de l'accès à un service par l'intermédiaire d'un réseau IP

LE(S) DEMANDEUR(S) :
FRANCE TELECOM

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		TRANSY	
Prénoms		Estelle	
Adresse	Rue	23, rue Victor Hugo	
	Code postal et ville	92130	ISSY LES MOULINEAUX
Société d'appartenance *(facultatif)*			
Nom		DELMOND	
Prénoms		Frédéric	
Adresse	Rue	80, rue de la Roquette	
	Code postal et ville	75011	PARIS
Société d'appartenance *(facultatif)*			
Nom		NGUYEN NGOC	
Prénoms		Sébastien	
Adresse	Rue	16, rue Fillassier	
	Code postal et ville	92140	CLAMART
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)
DE ROQUEMAUREL Bruno 02-0407

Levallois Perret, le 24.07.2003

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.